

CLAIMS

- 1 1. The method for mutual authentication of a first station and a second station,
2 comprising:
3 encrypting a particular data random key at the first station by first veiling the
4 particular data random key using a first conversion array seeded by a shared secret and
5 then encrypting the veiled particular data random key to produce a first encrypted key,
6 where access to the shared secret indicates authenticity of the first station;
7 sending a first message to the second station including the first encrypted key,
8 where the second station decrypts and unveils said particular data random key using the
9 shared secret, and where the second station encrypts the particular data random key by
10 first veiling a version of the particular data random key using a second conversion array
11 seeded by the shared secret and then encrypting the veiled version of the particular data
12 random key to produce a second encrypted key, and sends a second message to the first
13 station carrying the second encrypted key, where access to the shared secret indicates
14 authenticity of the second station; and
15 receiving the second message, and decrypting and unveiling the version of the
16 particular data random key at the first station.
- 1 2. The method of claim 1, including
2 encrypting an additional particular data random key at the first station by first
3 veiling the additional particular data random key using a first conversion array seeded by
4 an additional shared secret and then encrypting the veiled particular data random key to
5 produce a first additional encrypted key, where access to the additional shared secret
6 indicates authenticity of the first station;
7 sending a third message to the second station including the additional encrypted
8 key, where the second station decrypts and unveils said additional particular data random
9 key using the additional shared secret, and where the second station encrypts the
10 additional particular data random key by first veiling a version of the additional particular
11 data random key using a second conversion array seeded by the additional shared secret
12 and then encrypting the veiled version of the additional particular data random key to

13 produce a second additional encrypted key, and sends a second message to the first
14 station carrying the second additional encrypted key, where access to the additional
15 shared secret indicates authenticity of the second station; and
16 receiving the second message, and decrypting and unveiling the version of the
17 additional particular data random key at the first station.

1 3. The method of claim 2, wherein said additional particular data random key is the
2 same as the particular data random key.

1 4. The method of claim 1, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Y byte positions in an order, and
3 including instructions
4 generating one of the first and second conversion arrays using a random number
5 generator seeded by said shared secret to produce a pseudorandom number having X
6 values corresponding with respective sections of said X sections, the X values each being
7 between 1 and Y and identifying one of said Y byte positions, and
8 placing a byte of said random key in each of said X sections at the one of said Y
9 byte positions identified by the corresponding one of said X values.

1 5. The method of claim 1, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Z bit positions in an order, and
3 including
4 generating one of the first and second conversion arrays using a random number
5 generator seeded by said shared secret to produce a pseudorandom number having X
6 values corresponding with respective sections of said X sections, the X values each being
7 between 1 and Z and identifying one of said Z bit positions, and
8 placing a bit of said random key in each of said X sections at the one of said Z bit
9 positions identified by the corresponding one of said X values.

1 6. The method of claim 1, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Y byte positions in an order, each
3 of said Y byte positions including B bit positions in an order, and including
4 generating one of the first and second conversion arrays using a random number
5 generator seeded by said shared secret to produce a first pseudorandom number having X
6 values corresponding with respective sections of said X sections, the X values each being
7 between 1 and Y and identifying one of said Y byte positions,
8 using a random number generator seeded by said shared secret to produce a
9 second pseudorandom number having B values corresponding with respective bits in a
10 byte of said random key, the B values each being between 1 and B and identifying one of
11 said B bit positions,
12 placing a byte, including B bits, of said random key in each of said X sections at
13 the one of said Y byte positions identified by the corresponding one of said X values, and
14 mapping the B bits of said byte of said random key to said B bit positions
15 identified by the corresponding one of said B values.

1 7. The method of claim 1, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Y byte positions in an order, each
3 of said Y byte positions including B bit positions in an order, and including
4 generating one of the first and second conversion arrays using a random number
5 generator seeded by said shared secret to produce a first pseudorandom number having X
6 values corresponding with respective sections of said X sections, the X values each being
7 between 1 and Y and identifying one of said Y byte positions,
8 using a random number generator to produce a second pseudorandom number
9 having B values corresponding with respective bits in a byte of said random key, the B
10 values each being between 1 and B and identifying one of said B bit positions,
11 placing a byte, including B bits, of said random key in each of said X sections at
12 the one of said Y byte positions identified by the corresponding one of said X values, and
13 mapping the B bits of said byte of said random key to said B bit positions
14 identified by the corresponding one of said B values.

1 8. The method of claim 1, including presenting a use interface to the second station
2 from the first station carrying parameters of said first and second conversion arrays.

1 9. The method of claim 1, including executing an interactive exchange of messages
2 to deliver the particular data random key from the first station to the second station.

1 10. A data processing apparatus, comprising:

2 a processor, a communication interface adapted for connection to a
3 communication medium, and memory storing instructions for execution by the data
4 processor, the instructions including

5 logic to encrypt a particular data random key at the first station by first veiling the
6 particular data random key using a first conversion array seeded by a shared secret and
7 then encrypting the veiled particular data random key to produce a first encrypted key,
8 where access to the shared secret indicates authenticity of the first station;

9 logic to send a first message to the second station including the first encrypted
10 key, where the second station decrypts and unveils said particular data random key using
11 the shared secret, and where the second station encrypts the particular data random key
12 by first veiling a version of the particular data random key using a second conversion
13 array seeded by the shared secret and then encrypting the veiled version of the particular
14 data random key to produce a second encrypted key, and sends a second message to the
15 first station carrying the second encrypted key, where access to the shared secret indicates
16 authenticity of the second station; and

17 logic to receive the second message, and to decrypt and unveil the version of the
18 particular data random key at the first station.

1 11. The apparatus of claim 10, including logic to encrypt an additional particular data
2 random key at the first station by first veiling the additional particular data random key
3 using a first conversion array seeded by an additional shared secret and then encrypting
4 the veiled particular data random key to produce a first additional encrypted key, where
5 access to the additional shared secret indicates authenticity of the first station;

6 logic to send a third message to the second station including the additional
7 encrypted key, where the second station decrypts and unveils said additional particular
8 data random key using the additional shared secret, and where the second station encrypts
9 the additional particular data random key by first veiling a version of the additional
10 particular data random key using a second conversion array seeded by the additional
11 shared secret and then encrypting the veiled version of the additional particular data
12 random key to produce a second additional encrypted key, and sends a second message to
13 the first station carrying the second additional encrypted key, where access to the
14 additional shared secret indicates authenticity of the second station; and
15 logic to receive the second message, and to decrypt and unveil the version of the
16 additional particular data random key at the first station.

1 12. The apparatus of claim 11, wherein said additional particular data random key is
2 the same as the particular data random key.

1 13. The apparatus of claim 10, where the one of the first and second conversion
2 arrays comprises X sections, each of said X sections including Y byte positions in an
3 order, and including logic to
4 generate one of the first and second conversion arrays using a random number
5 generator seeded by said shared secret to produce a pseudorandom number having X
6 values corresponding with respective sections of said X sections, the X values each being
7 between 1 and Y and identifying one of said Y byte positions, and
8 to place a byte of said random key in each of said X sections at the one of said Y
9 byte positions identified by the corresponding one of said X values.

1 14. The apparatus of claim 10, where the one of the first and second conversion
2 arrays comprises X sections, each of said X sections including Z bit positions in an order,
3 and including logic to
4 generate one of the first and second conversion arrays using a random number
5 generator seeded by said shared secret to produce a pseudorandom number having X

6 values corresponding with respective sections of said X sections, the X values each being
 7 between 1 and Z and identifying one of said Z bit positions, and
 8 to place a bit of said random key in each of said X sections at the one of said Z bit
 9 positions identified by the corresponding one of said X values.

1 15. The apparatus of claim 10, where the one of the first and second conversion
 2 arrays comprises X sections, each of said X sections including Y byte positions in an
 3 order, each of said Y byte positions including B bit positions in an order, and including
 4 logic to
 5 generate one of the first and second conversion arrays using a random number
 6 generator seeded by said shared secret to produce a first pseudorandom number having X
 7 values corresponding with respective sections of said X sections, the X values each being
 8 between 1 and Y and identifying one of said Y byte positions,
 9 use a random number generator seeded by said shared secret to produce a second
 10 pseudorandom number having B values corresponding with respective bits in a byte of
 11 said random key, the B values each being between 1 and B and identifying one of said B
 12 bit positions,
 13 place a byte, including B bits, of said random key in each of said X sections at the
 14 one of said Y byte positions identified by the corresponding one of said X values, and
 15 map the B bits of said byte of said random key to said B bit positions identified by
 16 the corresponding one of said B values.

1 16. The apparatus of claim 10, where the one of the first and second conversion
 2 arrays comprises X sections, each of said X sections including Y byte positions in an
 3 order, each of said Y byte positions including B bit positions in an order, and including
 4 logic to
 5 generate one of the first and second conversion arrays using a random number
 6 generator seeded by said shared secret to produce a first pseudorandom number having X
 7 values corresponding with respective sections of said X sections, the X values each being
 8 between 1 and Y and identifying one of said Y byte positions,

9 use a random number generator to produce a second pseudorandom number
 10 having B values corresponding with respective bits in a byte of said random key, the B
 11 values each being between 1 and B and identifying one of said B bit positions,
 12 place a byte, including B bits, of said random key in each of said X sections at the
 13 one of said Y byte positions identified by the corresponding one of said X values, and
 14 map the B bits of said byte of said random key to said B bit positions identified by
 15 the corresponding one of said B values.

1 17. The apparatus of claim 10, including logic to present a user interface to the
 2 second station from the first station carrying parameters of said first and second
 3 conversion arrays.

1 18. The apparatus of claim 10, including logic to execute an interactive exchange of
 2 messages to deliver the particular data random key from the first station to the second
 3 station.

1 19. An article, comprising:
 2 machine readable data storage medium having computer program instructions
 3 stored therein for establishing a communication session on a communication medium
 4 between a first data processing station and a second data processing station having access
 5 to the communication medium, said instructions comprising
 6 logic to encrypt a particular data random key at the first station by first veiling the
 7 particular data random key using a first conversion array seeded by a shared secret and
 8 then encrypting the veiled particular data random key to produce a first encrypted key,
 9 where access to the shared secret indicates authenticity of the first station;
 10 logic to send a first message to the second station including the first encrypted
 11 key, where the second station decrypts and unveils said particular data random key using
 12 the shared secret, and where the second station encrypts the particular data random key
 13 by first veiling a version of the particular data random key using a second conversion
 14 array seeded by the shared secret and then encrypting the veiled version of the particular
 15 data random key to produce a second encrypted key, and sends a second message to the

16 first station carrying the second encrypted key, where access to the shared secret indicates
17 authenticity of the second station; and
18 logic to receive the second message, and to decrypt and unveil the version of the
19 particular data random key at the first station.

1 20. The article of claim 19, the instructions including logic to encrypt an additional
2 particular data random key at the first station by first veiling the additional particular data
3 random key using a first conversion array seeded by an additional shared secret and then
4 encrypting the veiled particular data random key to produce a first additional encrypted
5 key, where access to the additional shared secret indicates authenticity of the first station;
6 logic to send a third message to the second station including the additional
7 encrypted key, where the second station decrypts and unveils said additional particular
8 data random key using the additional shared secret, and where the second station encrypts
9 the additional particular data random key by first veiling a version of the additional
10 particular data random key using a second conversion array seeded by the additional
11 shared secret and then encrypting the veiled version of the additional particular data
12 random key to produce a second additional encrypted key, and sends a second message to
13 the first station carrying the second additional encrypted key, where access to the
14 additional shared secret indicates authenticity of the second station; and
15 logic to receive the second message, and to decrypt and unveil the version of the
16 additional particular data random key at the first station.

1 21. The article of claim 19, wherein said additional particular data random key is the
2 same as the particular data random key.

1 22. The article of claim 19, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Y byte positions in an order, and
3 the instructions include logic to
4 generate one of the first and second conversion arrays using a random number
5 generator seeded by said shared secret to produce a pseudorandom number having X

6 values corresponding with respective sections of said X sections, the X values each being
 7 between 1 and Y and identifying one of said Y byte positions, and
 8 to place a byte of said random key in each of said X sections at the one of said Y
 9 byte positions identified by the corresponding one of said X values.

1 23. The article of claim 19, where the one of the first and second conversion arrays
 2 comprises X sections, each of said X sections including Z bit positions in an order, and
 3 the instructions include logic to
 4 generate one of the first and second conversion arrays using a random number
 5 generator seeded by said shared secret to produce a pseudorandom number having X
 6 values corresponding with respective sections of said X sections, the X values each being
 7 between 1 and Z and identifying one of said Z bit positions, and
 8 to place a bit of said random key in each of said X sections at the one of said Z bit
 9 positions identified by the corresponding one of said X values.

1 24. The article of claim 19, where the one of the first and second conversion arrays
 2 comprises X sections, each of said X sections including Y byte positions in an order, each
 3 of said Y byte positions including B bit positions in an order, and the instructions include
 4 logic to
 5 generate one of the first and second conversion arrays using a random number
 6 generator seeded by said shared secret to produce a first pseudorandom number having X
 7 values corresponding with respective sections of said X sections, the X values each being
 8 between 1 and Y and identifying one of said Y byte positions,
 9 use a random number generator seeded by said shared secret to produce a second
 10 pseudorandom number having B values corresponding with respective bits in a byte of
 11 said random key, the B values each being between 1 and B and identifying one of said B
 12 bit positions,
 13 place a byte, including B bits, of said random key in each of said X sections at the
 14 one of said Y byte positions identified by the corresponding one of said X values, and
 15 map the B bits of said byte of said random key to said B bit positions identified by
 16 the corresponding one of said B values.

1 25. The article of claim 19, where the one of the first and second conversion arrays
2 comprises X sections, each of said X sections including Y byte positions in an order, each
3 of said Y byte positions including B bit positions in an order, and the instructions include
4 logic to
5 generate one of the first and second conversion arrays using a random number
6 generator seeded by said shared secret to produce a first pseudorandom number having X
7 values corresponding with respective sections of said X sections, the X values each being
8 between 1 and Y and identifying one of said Y byte positions,
9 use a random number generator to produce a second pseudorandom number
10 having B values corresponding with respective bits in a byte of said random key, the B
11 values each being between 1 and B and identifying one of said B bit positions,
12 place a byte, including B bits, of said random key in each of said X sections at the
13 one of said Y byte positions identified by the corresponding one of said X values, and
14 map the B bits of said byte of said random key to said B bit positions identified by
15 the corresponding one of said B values.

1 26. The article of claim 19, wherein the instructions include logic to present a user
2 interface to the second station from the first station carrying parameters of said first and
3 second conversion arrays.

1 27. The article of claim 19, wherein the instructions include logic to execute an
2 interactive exchange of messages to deliver the particular data random key from the first
3 station to the second station.